

# トラストサービスの現状と課題

## 第1回データ戦略タスクフォース

2020年10月23日

慶應義塾大学  
手塚 悟

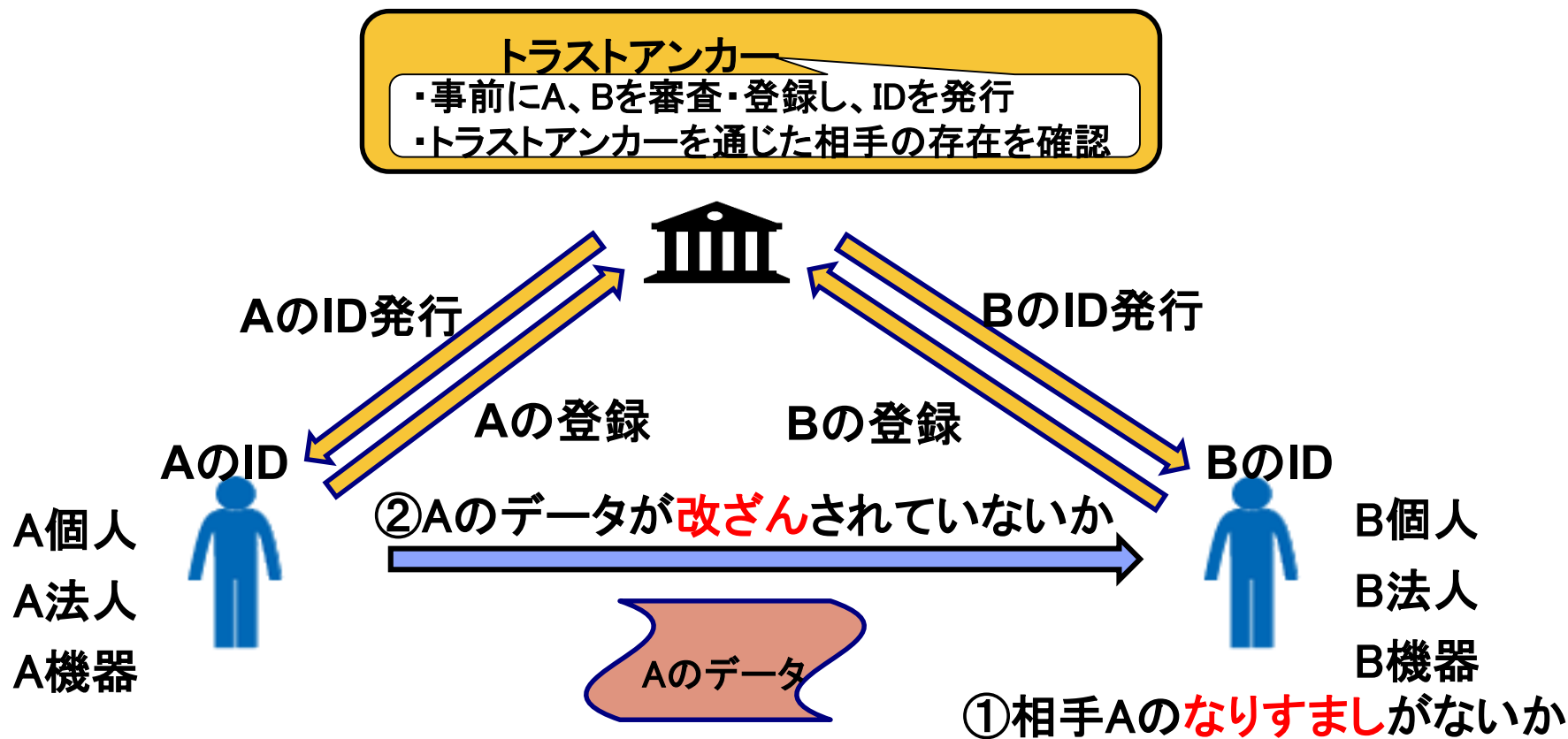
# 1. トラストサービスの意義

- Society5.0の中核となるデータ駆動型社会(Data-driven society)では、**良質、最新、正確かつ豊富なリアルデータが価値の源泉**となり、経済社会活動を支える最も重要な糧となることが見込まれる。これは、とりもなおさず、**経済社会を支える中核的な要素としてのデータの重要性が飛躍的に増大**することを意味する。
- このような様々な可能性を秘めるデータ駆動型社会においては、そのバックボーンとなる**データの真正性やデータ流通基盤の信頼性を確保**することが極めて大切となる。そのためには、**インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み(トラストサービス)の実現**に向けて、包括的な検討を加えることが必要となってくる。
- EUでは、**デジタル・シングル・マーケットを創設するために、その基盤を支える包括的なトラストサービスの法制化が進められており、このような国際的な動向も見据えながら、我が国におけるトラストサービスの在り方を検討することが必要**である。

## 2. トラストサービスにおけるトラスタンカーの概要

### ● トラスタンカーの役割

- IDの審査・登録・発行方法
- IDの格納・管理方法
- IDの連携方法



# 3. トラストサービスの機能

- ① 電子データを作成した本人として、ヒトの正当性を確認できる仕組み  
→ 電子署名(個人名の電子証明書)
- ② 電子データがある時刻に存在し、その時刻以降に当該データが改ざんされていないことを証明する仕組み  
→ タイムスタンプ
- ③ 電子データを発行した組織として、組織の正当性を確認できる仕組み  
→ eシール\*(組織名の電子証明書)
- ④ ウェブサイトが正当な企業等により開設されたものであるか確認する仕組み  
→ ウェブサイト認証
- ⑤ IoT時代における各種センサーから送信されるデータのなりすまし防止等のためモノの正当性を確認できる仕組み  
→ モノの正当性の認証
- ⑥ 送信・受信の正当性や送受信されるデータの完全性の確保を実現する仕組み  
→ eデリバリー

\*我が国において、電子文書の発信元の組織を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降、当該文書が改ざんされていないことを確認可能とする仕組みであって、電子文書の発信元が個人ではなく組織であるものを「eシール」と呼ぶことが一般的かは定かではないが、便宜上、EUにおける呼称である「eシール」を用いることとする。



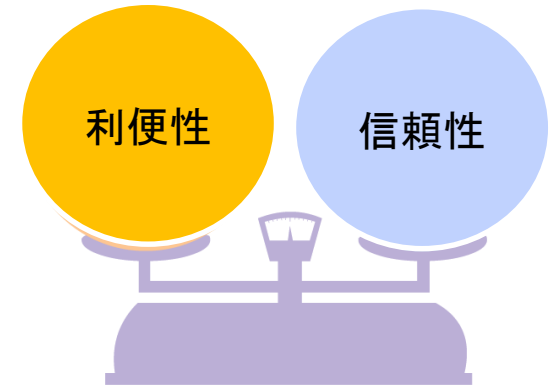
## 4. トラストサービスによる信頼性確保

- トラストサービスにおける**信頼の基点(トラスト・アンカー)**となるサービス・事業者の**客観的基準への適合性を、第三者が審査・評価・認定し、その結果を利用者に情報提供する仕組みが重要である。**
- **基準や認定の仕組みの整備・運用を行うサービス・事業者**については、各サービスの利用者が信頼を置けるサービスとするために、**必要かつ十分な客観的基準への適合性が求められる。**
- **国際的な通用性が重要と考えられるサービス**(例:電子署名、タイムスタンプ、eシール)については、**国の関与により信頼性を担保**することがより重要である。
- SSL/TLSで使われているサーバ認証については、現在**民間の関与により信頼性を担保**するものもある。
- 我が国の**トラストサービスの信頼性確保の方策検討**は、各サービスに関して**国の関与が良いのか、民間の関与が良いのか**を検討することが必要である。

# 5. トラストサービスの利便性と信頼性のバランス

## ● 紙の世界 → 電子の世界

- 書面 → 電子文書  
Paperless
- 対面 → 電子認証  
Electronic Authentication
- 押印  
(自署) → 電子署名  
Electronic Signature



- 「紙の世界」では、押印がコロナ渦でのオンライン完結型テレワークの妨げになっているので、**利便性のために廃止を検討中**である。
- 「電子の世界」では、単純に「紙の世界」と同様の利便性を追求するのは拙速であり、**信頼性を損ねるため、本末転倒になりかねない。**

# 6. トラストサービスの必要性

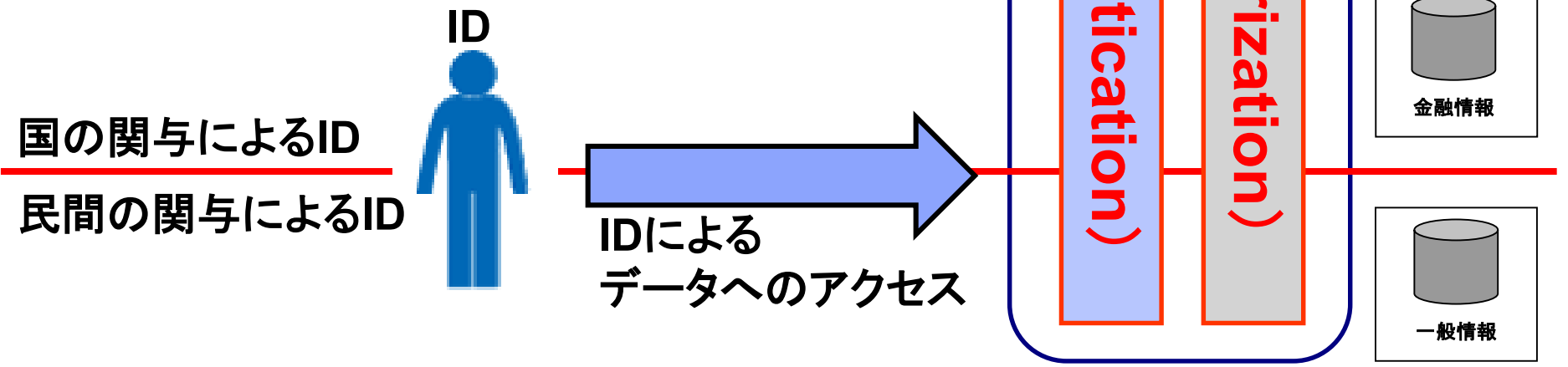
- 電子署名、タイムスタンプ、eシール等の各種トラストサービスが存在するが、これまで社会慣習として積み上げられてきた「紙の手交」や「対面」により醸成される安心感・信頼感などを、デジタルデータのみで提供するに至っていないのが問題である。
- 目指すべき社会像に向けては、利用者がデジタルデータを安心して信頼できる環境が必要。そのため、各種トラストサービスの位置づけを明確化する必要がある。
- トラストを担保・確認するためには、一般的にデータに含まれるものは「意思・伝達」、「事実・情報」、「時刻・存在」であり、これらが間違っていないこと(真正性)、改ざんされていないこと(完全性)の証明が必要である。

	完全性		
真正性		生成時から 非改ざん	ある時点から 非改ざん
意思 (メール等)		①意思表示の証明 ・限定的な自然人による証明	・当事者が振り返るのであれば「①意思表示の証明」、 ・第三者が振り返るのであれば「②発行元証明」 に包含。
事実 (観測データ等) ・ 情報		②発行元証明 ・生成者による証明 ・自明でない限り、生成手段を明示	③存在証明 ・任意の者による証明 ・確認の時点の証明が必要

# 7. トラストサービスにおける利用者証明の利活用

- IDとDataの分類によるデータへのアクセス制御が必要
  - ID: 審査・登録
  - Data: データ区分

トラストアンカーの審査・登録によるID発行





# 8. トラストサービスにおける国際相互連携の概要

## ●「自由と信頼」のルールに基づくデータ流通圏と国際相互連携

- Japan-EU Digital Trade

日EU経済連携協定: 2019年2月1日 発効

- Japan-US Digital Trade

日米デジタル貿易協定: 2019年12月13日 公布

